

Локальные и глобальные методы в арифметике

А.А.Панчишкин

Аннотация

Пусть p – простое число. Обсуждаются методы решения сравнений по модулю p^n с помощью p -адических чисел, аналогичные методам решения уравнений в действительных числах. Приведены примеры связи локальных и глобальных методов решения в арифметике, а также примеры компьютерных вычислений с p -адическими числами и алгебраическими кривыми.

Содержание

1	Введение	2
2	p-адические числа и сравнения	2
2.1	Приложения p -адических чисел к решению сравнений.	7
3	Диофантовы системы линейных уравнений и сравнений	8
3.1	Вычисления с классами вычетов.	8
3.2	Уравнение $ax + by = c$	9
3.3	Системы линейных уравнений с целыми коэффициентами	10
4	Уравнения второй степени.	11
4.1	Квадратичные формы и квадратики	11
4.2	Принцип Минковского—Хассе для квадратичных форм.	13
4.3	Символ Гильберта.	14
5	Кубические уравнения и эллиптические кривые	16
5.1	Проблема существования рационального решения.	16
5.2	Сложение точек на кубической кривой.	17
5.3	Строение группы рациональных точек на кубической кривой	19
5.4	Кубические сравнения по простому модулю.	20
5.5	От сравнений к рациональным точкам: гипотеза Бёрча и Суиннертона–Дайера	22
5.5.1	Гипотеза БСД	22
5.5.2	Что известно о гипотезе БСД	22
5.5.3	Вычисления с эллиптическими кривыми	23
5.5.4	С чего начать вычисления на PARI-GP	23
5.5.5	Как вычислить $L(E, s)$ на компьютере	23
5.5.6	Приближённое вычисление ранга	24

1 Введение

Статья основана на материалах лекций автора в Институте Фурье (Гренобль, Франция), в Эколь Нормаль (Лион, Франция), а также на материалах спецкурсов на мех-мате МГУ в 1979-1991 и в 2001.

В статье обсуждаются следующие темы:

- 1) p -адические числа и сравнения. Диофантовы системы линейных уравнений и сравнений
- 2) Принцип Минковского—Хассе для квадратичных форм
- 3) Символ Гильберта и его вычисление
- 4) Кубические уравнения и эллиптические кривые
- 5) От сравнений к рациональным точкам: гипотеза Бёрча и Суиннертона—Дайера

2 p -адические числа и сравнения

Идея расширения поля \mathbb{Q} в теории чисел встречается в различных вариантах. Например, вложение, $\mathbb{Q} \subset \mathbb{R}$ часто дает полезные необходимые условия существования решений диофантовых уравнений над \mathbb{Q} и над \mathbb{Z} . Важное свойство поля \mathbb{R} его полнота: любая фундаментальная последовательность (последовательность Коши): $\{\alpha_n\}_{n=1}^\infty$ в \mathbb{R} имеет предел α . Фундаментальность означает, что для произвольного $\varepsilon > 0$ малы абсолютные величины $|\alpha_n - \alpha_m| < \varepsilon$ для всех n и m больших некоторого натурального числа $N = N(\varepsilon)$. Кроме того, все элементы \mathbb{R} являются пределами фундаментальных последовательностей $\{\alpha_n\}_{n=1}^\infty$ с $\alpha_n \in \mathbb{Q}$.

Аналогичная конструкция существует и для всех p -адических нормирований $|\cdot|_p$ поля \mathbb{Q} :

$$\begin{aligned} |\cdot|_p : \mathbb{Q} &\rightarrow \mathbb{R}_{\geq 0} = \{x \in \mathbb{R} \mid x \geq 0\} \\ |a/b|_p &= p^{\text{ord}_p b - \text{ord}_p a}, \quad |0|_p = 0, \end{aligned}$$

где $\text{ord}_p a$ наивысшая степень числа p делящая целое число a . Эта общая конструкция «присоединения пределов фундаментальных последовательностей» относительно некоторого нормирования $|\cdot|$ поля k называется пополнением. В результате получается поле \hat{k} , с нормированием, также обозначаемом $|\cdot|$ причем поле \hat{k} — полное, а k однозначно вкладывается в \hat{k} в качестве всюду плотного подполя с сохранением нормирования, см. [BS85], [Kob80].

Согласно теореме Островского, все нормирования поля \mathbb{Q} сводятся либо к абсолютной величине, либо к p -адическому нормированию $|\cdot|_p$ (с точностью до эквивалентности). Поэтому все пополнения поля \mathbb{Q} это либо поле действительных чисел, \mathbb{R} , либо поля \mathbb{Q}_p p -адических чисел. Использование всевозможных вложений $\mathbb{Q} \hookrightarrow \mathbb{R}$ и $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ (p —простое число) часто значительно упрощает ситуацию в арифметических задачах. Замечательный пример дает *теорема Минковского—Хассе* (см.[BS85], глава 1). Уравнение

$$Q(x_1, x_2, \dots, x_n) = 0, \tag{2.1}$$

заданное квадратичной формой $Q(x_1, x_2, \dots, x_n) = \sum_{i,j} a_{ij} x_i x_j$, $a_{ij} \in \mathbb{Q}$, имеет нетривиальное решение в рациональных числах в том и только в том случае, когда оно нетривиально разрешимо над \mathbb{R} и над \mathbb{Q}_p для всех простых чисел p . Для нахождения решений уравнений над \mathbb{Q}_p можно эффективно применять приемы, взятые по аналогии из анализа над \mathbb{R} , такие, как

«метод касательных Ньютона» (“*Newton - Raphson algorithm*”), который в p -адическом случае известен как *лемма Гензеля*, (*Hensel's lemma*).

Наиболее простым способом можно ввести p -адические числа как выражения вида

$$\alpha = a_m p^m + a_{m+1} p^{m+1} + \dots, \quad (2.2)$$

где $a_i \in \{0, 1, \dots, p-1\}$ —цифры (по основанию p , а $m \in \mathbb{Z}$. Удобно записывать α в виде последовательности цифр, бесконечной влево:

$$\alpha = \begin{cases} \cdots a_{m+1} a_m \overbrace{000 \dots 0}^{m-1 \text{ zeros}}_{(p)}, & \text{if } m \geq 0, \\ \cdots a_1 a_0 . a_{-1} \cdots a_{m(p)}, & \text{if } m < 0. \end{cases}$$

Эти выражения образуют поле, в котором операции выполняются так же, как для натуральных чисел $n = a_0 + a_1 p + \dots a_r p^r$, записанных по основанию p . Следовательно, в этом поле лежат натуральные, а потому и все рациональные числа. Например,

$$-1 = \frac{p-1}{1-p} = (p-1) + (p-1)p + (p-1)p^2 + \dots = \cdots (p-1)(p-1)_{(p)};$$

$$\frac{-a_0}{p-1} = a_0 + a_0 p + a_0 p^2 + \dots = \cdots a_0 a_0 a_0_{(p)}.$$

Если $n \in \mathbb{N}$, то выражение для $-n = n \cdot (-1)$ вида (2.2) получается, если перемножить указанные выражения для n и для -1 . Вообще, если $\alpha \in \mathbb{Q}$ то запишем $\alpha = c - \frac{a}{b}$, где $a, c \in \mathbb{Z}$, $b \in \mathbb{N}$, $0 \leq a < b$, т.е. a/b правильная дробь. Тогда по элементарной теореме Эйлера, $p^{\varphi(b)} - 1 = bu$, $u \in \mathbb{N}$. Поэтому

$$-\frac{a}{b} = \frac{au}{1 - p^{\varphi(b)}},$$

и $au < bu = p^r - 1$, $r = \varphi(b)$. Теперь мы видим, что запись по основанию p числа au имеет вид $a_{r-1} \cdots a_0_{(p)}$, следовательно, выражение (2.2) для числа α получается как сумма выражения для $c \in \mathbb{N}$ и

$$-\frac{a}{b} = \cdots a_0 \overbrace{a_{r-1} \cdots a_0}^{r \text{ digits}} \cdots a_0 \overbrace{a_{r-1} \cdots a_0}^{r \text{ digits}}_{(p)}.$$

Например, для $p = 5$ имеем

$$\frac{9}{7} = 2 - \frac{5}{7} = 2 + \frac{5 \cdot 2232}{1 - 5^6} \quad c = 2 \quad a = 5, \quad b = 7,$$

причем

$$2232 = 32412_{(5)} = 3 \cdot 5^4 + 2 \cdot 5^3 + 4 \cdot 5^2 + 1 \cdot 5 + 2,$$

поэтому

$$\frac{9}{7} = \cdots \overbrace{324120324120324122}_{(5)}.$$

Нетрудно проверить, что пополнение поля \mathbb{Q} относительно p -адической метрики $|\cdot|_p$ отождествляется с полем « p -адических разложений» вида (2.2). При этом $|\alpha|_p = p^m$ где в выражении (2.2) для α имеем $a_m \neq 0$ (см. [Kob80]).

p -адические разложения можно рассматривать как аналоги разложения функции f переменной x в окрестности точки a по степеням $(x - a)$, причём p является аналогом $(x - a)$:

Вычисление с PARI-GP

```
gp > forprime(p=2,163,print("p=",p,", ""9/7="9/7+0(p^6)))
p=2,9/7=1 + 2 + 2^2 + 2^3 + 2^5 + 0(2^6)
p=3,9/7=3^2 + 3^3 + 2*3^5 + 0(3^6)
p=5,9/7=2 + 2*5 + 5^2 + 4*5^3 + 2*5^4 + 3*5^5 + 0(5^6)
p=7,9/7=2*7^-1 + 1 + 0(7^6)
p=11,9/7=6 + 9*11 + 7*11^2 + 4*11^3 + 9*11^4 + 7*11^5 + 0(11^6)
p=13,9/7=5 + 9*13 + 3*13^2 + 9*13^3 + 3*13^4 + 9*13^5 + 0(13^6)
p=17,9/7=11 + 14*17 + 4*17^2 + 7*17^3 + 2*17^4 + 12*17^5 + 0(17^6)
p=19,9/7=4 + 8*19 + 5*19^2 + 16*19^3 + 10*19^4 + 13*19^5 + 0(19^6)
p=23,9/7=21 + 9*23 + 16*23^2 + 19*23^3 + 9*23^4 + 16*23^5 + 0(23^6)
p=29,9/7=22 + 20*29 + 20*29^2 + 20*29^3 + 20*29^4 + 20*29^5 + 0(29^6)
p=31,9/7=19 + 26*31 + 8*31^2 + 13*31^3 + 4*31^4 + 22*31^5 + 0(31^6)
p=37,9/7=33 + 15*37 + 26*37^2 + 31*37^3 + 15*37^4 + 26*37^5 + 0(37^6)
p=41,9/7=13 + 29*41 + 11*41^2 + 29*41^3 + 11*41^4 + 29*41^5 + 0(41^6)
p=43,9/7=32 + 30*43 + 30*43^2 + 30*43^3 + 30*43^4 + 30*43^5 + 0(43^6)
p=47,9/7=8 + 20*47 + 13*47^2 + 40*47^3 + 26*47^4 + 33*47^5 + 0(47^6)
p=53,9/7=24 + 45*53 + 37*53^2 + 22*53^3 + 45*53^4 + 37*53^5 + 0(53^6)
p=59,9/7=35 + 50*59 + 16*59^2 + 25*59^3 + 8*59^4 + 42*59^5 + 0(59^6)
p=61,9/7=10 + 26*61 + 17*61^2 + 52*61^3 + 34*61^4 + 43*61^5 + 0(61^6)
p=67,9/7=30 + 57*67 + 47*67^2 + 28*67^3 + 57*67^4 + 47*67^5 + 0(67^6)
p=71,9/7=52 + 50*71 + 50*71^2 + 50*71^3 + 50*71^4 + 50*71^5 + 0(71^6)
p=73,9/7=43 + 62*73 + 20*73^2 + 31*73^3 + 10*73^4 + 52*73^5 + 0(73^6)
p=79,9/7=69 + 33*79 + 56*79^2 + 67*79^3 + 33*79^4 + 56*79^5 + 0(79^6)
p=83,9/7=25 + 59*83 + 23*83^2 + 59*83^3 + 23*83^4 + 59*83^5 + 0(83^6)
p=89,9/7=14 + 38*89 + 25*89^2 + 76*89^3 + 50*89^4 + 63*89^5 + 0(89^6)
p=97,9/7=29 + 69*97 + 27*97^2 + 69*97^3 + 27*97^4 + 69*97^5 + 0(97^6)
p=101,9/7=59 + 86*101 + 28*101^2 + 43*101^3 + 14*101^4 + 72*101^5 + 0(101^6)
p=103,9/7=16 + 44*103 + 29*103^2 + 88*103^3 + 58*103^4 + 73*103^5 + 0(103^6)
p=107,9/7=93 + 45*107 + 76*107^2 + 91*107^3 + 45*107^4 + 76*107^5 + 0(107^6)
p=109,9/7=48 + 93*109 + 77*109^2 + 46*109^3 + 93*109^4 + 77*109^5 + 0(109^6)
p=113,9/7=82 + 80*113 + 80*113^2 + 80*113^3 + 80*113^4 + 80*113^5 + 0(113^6)
p=127,9/7=92 + 90*127 + 90*127^2 + 90*127^3 + 90*127^4 + 90*127^5 + 0(127^6)
p=131,9/7=20 + 56*131 + 37*131^2 + 112*131^3 + 74*131^4 + 93*131^5 + 0(131^6)
p=137,9/7=60 + 117*137 + 97*137^2 + 58*137^3 + 117*137^4 + 97*137^5 + 0(137^6)
p=139,9/7=41 + 99*139 + 39*139^2 + 99*139^3 + 39*139^4 + 99*139^5 + 0(139^6)
p=149,9/7=129 + 63*149 + 106*149^2 + 127*149^3 + 63*149^4 + 106*149^5 + 0(149^6)
```

```
p=151,9/7=66 + 129*151 + 107*151^2 + 64*151^3 + 129*151^4 + 107*151^5 + 0(151^6)
```

```
p=157,9/7=91 + 134*157 + 44*157^2 + 67*157^3 + 22*157^4 + 112*157^5 + 0(157^6)
```

```
p=163,9/7=141 + 69*163 + 116*163^2 + 139*163^3 + 69*163^4 + 116*163^5 + 0(163^6)
```

Любопытно сравнить разложения (2.2) «бесконечные влево», с разложениями действительных чисел $\alpha \in \mathbb{R}$, «бесконечными вправо»:

$$\alpha = a_m a_{m-1} \cdots a_0 . a_{-1} \cdots = a_m 10^m + a_{m-1} 10^{m-1} + \cdots a_0 + a_{-1} 10^{-1} + \cdots, \quad (2.3)$$

где $a_i \in \{0, 1, \dots, 9\}$ —цифры, а $a_m \neq 0$. Разложения такого типа по любому натуральному основанию приводят к одному и тому же полю \mathbb{R} , при этом они неоднозначны, к примеру, $2.000\dots = 1.999\dots$. Разложения (2.3) можно рассматривать как аналоги разложения в окрестности точки $p = \infty$, причём $p = \infty$ является аналогом x^{-1} .

Разложения (2.2) в p -адическом случае всегда однозначно определены, что создает дополнительные вычислительные удобства.

Поле \mathbb{Q}_p является *полным метрическим пространством* с топологией, определенной системой «открытых дисков» вида:

$$U_a(r) = \{x \mid |x - a| < r\} \quad (x, a \in \mathbb{Q}_p, r > 0)$$

(или «замкнутых дисков» $D_a(r) = \{x \mid |x - a| \leq r\}$). При этом $U_a(r)$ и $D_a(r)$ являются открыто-замкнутыми множествами с топологической точки зрения \mathbb{Q}_p .

Важное топологическое свойство поля \mathbb{Q}_p —его *локальная компактность*: все диски конечного радиуса компактны. В этом проще всего убедиться на языке последовательностей, показав, что каждая последовательность $\{\alpha_n\}_{n=1}^\infty$ элементов диска $\alpha_n \in D_a(r)$ имеет в этом же диске предельную точку. Эта предельная точка легко ищется с помощью *p -адических цифр* (2.2) последовательно, справа налево, и используется тот факт, что у всех элементов $\alpha_n \in D_a(r)$ число знаков «после запятой» ограничено фиксированным числом. В частности, диск

$$\mathbb{Z}_p = D_0(1) = \{x \mid |x|_p \leq 1\} = \{x = a_0 + a_1p + a_2p^2 + \dots\}$$

— это компактное топологическое кольцо, элементы которого называются целыми p -адическими числами, при этом \mathbb{Z}_p совпадает с замыканием множества обычных целых чисел \mathbb{Z} в \mathbb{Q}_p . Кольцо \mathbb{Z}_p является локальным, т. е. имеет единственный максимальный идеал $p\mathbb{Z}_p = U_0(1)$ с полем вычетов $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$. Множество обратимых элементов единиц кольца \mathbb{Z}_p — это

$$\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus p\mathbb{Z}_p = \{x \mid |x|_p = 1\} = \{x = a_0 + a_1p + a_2p^2 + \dots \mid a_0 \neq 0\}.$$

Для каждого элемента $x \in \mathbb{Z}_p$ определен его представитель Тейхмюллера

$$\omega(x) = \lim_{n \rightarrow \infty} x^{p^n}.$$

(предел всегда существует и удовлетворяет уравнению: $\omega(x)^p = \omega(x)$, и справедливо сравнение $\omega(x) \equiv x \pmod{p}$. Например, для $p = 5$ имеем

$$\begin{aligned} \omega(1) &= 1; \\ \omega(2) &= 2 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 \dots; \\ \omega(3) &= 3 + 3 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + 1 \cdot 5^4 + \dots; \\ \omega(4) &= 4 + 4 \cdot 5 + 4 \cdot 5^2 + 4 \cdot 5^3 + 4 \cdot 5^4 + \dots = -1; \\ \omega(5) &= 0. \end{aligned}$$

Кольцо \mathbb{Z}_p можно описать также как проективный предел

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

колец $A_n = \mathbb{Z}/p^n\mathbb{Z}$ относительно гомоморфизмов редукции по модулю p^{n-1} $\varphi_n : A_n \rightarrow A_{n-1}$. Последовательность

$$\dots \xrightarrow{\varphi_{n+1}} A_n \xrightarrow{\varphi_n} A_{n-1} \xrightarrow{\varphi_{n-1}} \dots \xrightarrow{\varphi_3} A_2 \xrightarrow{\varphi_2} A_1 \quad (2.4)$$

образует проективную систему, занумерованную целыми числами $n \geq 1$. Проективный предел системы (2.4)—это кольцо

$$\varprojlim_n A_n$$

со следующим универсальным свойством: однозначно определены такие гомоморфизмы проекции

$$\pi_n : \varprojlim_n A_n \rightarrow A_n,$$

что для произвольного кольца B и системы гомоморфизмов $\psi_n : B \rightarrow A_n$ согласованных друг с другом условием: $\psi_{n-1} = \varphi_n \circ \psi_n$ for $n \geq 2$, существует единственный гомоморфизм $\psi : B \rightarrow A$ для которого $\psi_n = \pi_n \psi$ (см. [Kob80], [Se70]). Для кольца A построение гомоморфизмов проекции и проверка универсального свойства непосредственно вытекают из записи его элементов с помощью «цифр» (2.2).

Аналогично,

$$\mathbb{Z}_p^\times = \varprojlim_n (\mathbb{Z}/p^n \mathbb{Z})^\times,$$

(проективный предел групп). Для описания группы \mathbb{Q}_p^\times положим $\nu = 1$ если $p > 2$ и $\nu = 2$ если $p = 2$, и определим

$$U = U_p = \{x \in \mathbb{Z}_p \mid x \equiv 1 \pmod{p^\nu}\}.$$

Тогда $U \xrightarrow{\sim} \mathbb{Z}_p$ (изоморфизм мультипликативной и аддитивной групп) U_p и \mathbb{Z}_p . Для построения этого изоморфизма заметим, что

$$U \xrightarrow{\sim} \varprojlim_n U/U^{p^n}$$

и определим изоморфизмы конечных групп

$$\alpha_{p^n} : U/U^{p^n} \xrightarrow{\sim} \mathbb{Z}/p^n \mathbb{Z},$$

положив

$$\alpha_{p^n}((1 + p^\nu)^a) = a \pmod{p^n} \quad (a \in \mathbb{Z}). \quad (2.5)$$

Простая проверка показывает, что отображения (2.5) корректно определены и являются изоморфизмами. Таким образом, группа U —это топологическая циклическая группа, в качестве образующей которой можно взять $1 + p^\nu$. Другое доказательство следует из свойств функции, определенной степенным рядом

$$\log(1 + x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n},$$

которая задаёт изоморфизм из U на $p\mathbb{Z}_p$

Проверяется, что справедливы разложения

$$\mathbb{Q}_p^\times = p^\mathbb{Z} \times \mathbb{Z}_p^\times, \quad \mathbb{Z}_p^\times \cong (\mathbb{Z}/p^\nu \mathbb{Z})^\times \times U. \quad (2.6)$$

2.1 Приложения p -адических чисел к решению сравнений.

Возникновение p -адических чисел в работах Гензеля было тесно связано с проблемой решения сравнений по модулю p^n , а применение их к теории квадратичных форм его учеником Хассе привело к элегантной формулировке теории квадратичных форм над рациональными числами, не использующей рассмотрений в кольцах вычетов вида $\mathbb{Z}/p^n\mathbb{Z}$, работать с которыми затруднительно из-за наличия делителей нуля в $\mathbb{Z}/p^n\mathbb{Z}$. Из представления кольца \mathbb{Z}_p в виде проективного предела $\mathbb{Z}/p^n\mathbb{Z}$,

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

вытекает, что если $f(x_1, \dots, x_n) \in \mathbb{Z}_p[x_1, \dots, x_n]$, то сравнения

$$f(x_1, \dots, x_n) \equiv 0 \pmod{p^n}$$

разрешимы при любом $n \geq 1$ тогда и только тогда, когда уравнение

$$f(x_1, \dots, x_n) = 0$$

разрешимо в целых p -адических числах. Эти решения в \mathbb{Z}_p можно находить с помощью p -адического варианта метода касательных Ньютона (*“Newton - Raphson algorithm”*).

Теорема 2.1 (лемма Гензеля) Пусть $f(x) \in \mathbb{Z}_p[x]$ – многочлен одной переменной x , $f'(x) \in \mathbb{Z}_p[x]$ – его формальная производная, и для некоторого $\alpha_0 \in \mathbb{Z}_p$ выполнено начальное условие

$$|f(\alpha_0)/f'(\alpha_0)^2|_p < 1 \quad (2.7)$$

Тогда существует единственное такое $\alpha \in \mathbb{Z}_p$, что

$$f(\alpha) = 0, \quad |\alpha - \alpha_0| < 1.$$

Доказательство проводится с помощью рассмотрения последовательности:

$$\alpha_n = \alpha_{n-1} - \frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})}.$$

С учетом формального разложения Тейлора многочлена $f(x)$ в точке $x = \alpha_{n-1}$ проверяется, что последовательность фундаментальна, а её предел α обладает всеми необходимыми свойствами (см. [BS85], [Se70]).

Например, если $f(x) = x^{p-1} - 1$, то любое $\alpha_0 \in \{1, 2, \dots, p-1\}$ удовлетворяет условию $|f(\alpha_0)|_p < 1$, в то время как $f'(\alpha_0) = (p-1)\alpha_0^{p-2} \not\equiv 0 \pmod{p}$, поэтому начальное условие (2.7) выполнено. Корень α совпадает при этом с единственным представителем Тейхмюллера числа α_0 : $\alpha = \omega(\alpha_0)$.

Описанный метод применим и к многочленам многих переменных, но уже без сохранения единственности находимого решения, (см. [BS85], [Kob80], [Se70]).

Еще одно приложение леммы Гензеля связано с описанием квадратов поля \mathbb{Q}_p : для произвольного элемента

$$\alpha = p^m \cdot v \in \mathbb{Q}_p \quad (m \in \mathbb{Z}, v \in \mathbb{Z}_p^\times),$$

свойство α быть квадратом в \mathbb{Q}_p равносильно тому, что

а) если $p > 2$, то $m \in 2\mathbb{Z}$, а $\bar{v} = v \bmod p \in (\mathbb{Z}/p\mathbb{Z})^{\times 2}$ (т.е. $\left(\frac{\bar{v}}{p}\right) = 1$, где $\left(\frac{\bar{v}}{p}\right)$ — символ Лежандра

б) если $p = 2$, то $m \in 2\mathbb{Z}$, а $v \equiv 1 \bmod 8$.

Разрешимость уравнения $x^2 = \alpha$ в \mathbb{Q}_p в условиях а) и б) выводится из леммы Гензеля, а необходимость их вытекает из более тривиальных рассмотрений по модулю p и по модулю 8.

Как следствие мы получаем, что факторгруппа $\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$

а) при $p > 2$ изоморфна $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ с системой представителей $\{1, p, v, pv\}$, $\left(\frac{\bar{v}}{p}\right) = -1$;

б) при $p = 2$ изоморфна $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ с системой представителей $\{\pm 1, \pm 5, \pm 2, \pm 10\}$.

3 Диофантовы системы линейных уравнений и сравнений

3.1 Вычисления с классами вычетов.

С точки зрения алгебры, множество целых чисел \mathbb{Z} является коммутативным ассоциативным кольцом с единицей, т. е. множеством с двумя коммутативными и ассоциативными операциями (сложение и умножение), связанными друг с другом законом дистрибутивности. Понятие делимости в кольцах связано с понятием идеала. Идеалом I в коммутативном ассоциативном кольце R называется подмножество с $RIR \subset I$.

Идеал вида $I = aR$, $a \in A$ называется главным идеалом, порожденным элементом (a) . Тогда отношение делимости $a|b$ в кольце R равносильно включению соответствующих главных идеалов:

$$(b) \subset (a) \quad \text{или} \quad b \in (a).$$

В кольце \mathbb{Z} деление с остатком на наименьший положительный элемент в идеале $I \neq 0$ показывает, что все идеалы главные, т. е. всякий ненулевой идеал I имеет вид $(N) = N\mathbb{Z}$ для натуральных чисел $N > 1$. При этом идеалы, максимальные по включению, в точности соответствуют простым числам. Остатки от деления на N подразделяют все целые числа на непересекающиеся классы

$$\bar{a} = a + N\mathbb{Z}, \quad 0 \leq a \leq N - 1,$$

множество которых также образует кольцо, обозначаемое

$$\mathbb{Z}/N\mathbb{Z} = \mathbb{Z}/(N) = \{\bar{0}, \bar{1}, \dots, \overline{N-1}\},$$

и пишется $a \equiv b \pmod{N}$ вместо $\bar{a} = \bar{b}$. Часто в задачах теории чисел вычисления в кольце \mathbb{Z} можно сводить к вычислениям в кольце вычетов $\mathbb{Z}/N\mathbb{Z}$. Это доставляет ряд удобств, например, на многие элементы из $\mathbb{Z}/N\mathbb{Z}$ можно делить, оставаясь в пределах этого кольца (в отличие от целых чисел, где всегда определено только деление на ± 1). Действительно, если число a взаимно просто с N , т. е. $\gcd(a, N) = 1$, класс \bar{a} обратим, так как в этом случае существуют такие целые числа x, y , что $ax + Ny = 1$, поэтому $\bar{a} \cdot \bar{x} = \bar{1}$. Так получаются все обратимые элементы кольца вычетов $\mathbb{Z}/N\mathbb{Z}$ которые образуют группу по умножению, обозначаемую $(\mathbb{Z}/N\mathbb{Z})^\times$. Порядок этой группы, обозначается $\varphi(N)$ (функция Эйлера). Название происходит из обобщения малой теоремы Ферма, принадлежащего Эйлеру:

$$a^{\varphi(N)} \equiv 1 \pmod{N} \tag{3.8}$$

для всех таких элементов a , что $\gcd(a, N) = 1$, т.е. $\bar{a}^{\varphi(N)} = \bar{1}$ для таких элементов \bar{a} в кольце $\mathbb{Z}/N\mathbb{Z}$.

Доказательство Эйлера, применимое к любой конечной абелевой группе порядка f , показывает, что порядок любого элемента a делит f . Умножение на a является перестановкой множества элементов конечной абелевой группы (а данном случае группы $(\mathbb{Z}/N\mathbb{Z})^\times$ порядка $f = \varphi(N)$). Произведение всех элементов группы умножается на a^f при этой перестановке. Поэтому $a^f = 1$.

Если число N разложено в произведение $N = N_1 N_2 \dots N_k$ попарно взаимно простых чисел N_i , то имеется разложение

$$\mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/N_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/N_k\mathbb{Z}. \quad (3.9)$$

в прямое произведение колец, что эквивалентно китайской теореме об остатках: для любых вычетов $a_i \bmod N_i$, $i = 1, \dots, k$ найдется такое целое число a , что $a \equiv a_i \bmod N_i$ для всех i . Практический поиск числа a можно быстро осуществить, применяя повторно алгоритм Евклида. Положим $M_i = N/N_i$, тогда числа M_i и N_i по условию взаимно просты, и существуют такие целые числа X_i что $X_i M_i \equiv 1 \bmod N_i$. Положим теперь

$$a = \sum_{i=1}^k a_i X_i M_i. \quad (3.10)$$

Следовательно, число a искомое. Кроме того, из разложения (3.9) вытекает и разложение мультипликативной группы:

$$(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/N_1\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/N_k\mathbb{Z})^\times, \quad (3.11)$$

из которого, в частности, следует, что $\varphi(N) = \varphi(N_1) \dots \varphi(N_k)$. Поскольку для простого числа p имеем $\varphi(p^a) = p^{a-1}(p-1)$, мы находим $\varphi(N)$ исходя из разложения числа N .

В специальном случае, когда $N = q$ простое число, кольцо вычетов $\mathbb{Z}/N\mathbb{Z}$ является полем: в нем обратим любой элемент, отличный от нуля.

3.2 Уравнение $ax + by = c$

В этом параграфе все буквы (коэффициенты и неизвестные в уравнениях) означают целые числа. Множество

$$I(a, b) = \{c \mid \text{уравнение } ax + by = c \text{ разрешимо (в целых числах)}\}$$

является идеалом кольца \mathbb{Z} и поэтому $I(a, b)$ имеет вид $d\mathbb{Z}$, где $d = (a, b)$ — наибольший общий делитель. Таким образом, уравнение

$$ax + by = c \quad (3.12)$$

разрешимо, только если d делит c . Конкретное решение находится с помощью алгоритма Евклида: если X, Y с $aX + bY = d$ то числа $x_0 = eX, y_0 = eY$ удовлетворяют уравнению, где $e = c/d$. Теперь мы получили все целочисленные решения:

$$x = x_0 + (b/d)t, \quad y = y_0 - (a/d)t,$$

где t произвольное целое число.

Уравнение (3.12) дает первый пример общей проблемы: для системы уравнений, заданной целочисленными многочленами

$$F_1(x_1, \dots, x_n) = 0, \quad \dots, \quad F_m(x_1, \dots, x_n) = 0 \quad (3.13)$$

найти все целочисленные (или все рациональные) решения. Для уравнения (3.12) задача нахождения рациональных решений тривиальна. Если в системе (3.13) все уравнения $F_i = 0$ линейные, то и для нее все рациональные решения легко находятся последовательным исключением неизвестных (например, по методу Гаусса).

3.3 Системы линейных уравнений с целыми коэффициентами

Опишем общий прием нахождения всех целочисленных решений системы (целочисленных) линейных уравнений, записанной в матричной форме

$$Ax = b, \quad (3.14)$$

где

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \ddots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \in M_{m,n}(\mathbb{Z}), \quad x = \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}, \quad b = \begin{pmatrix} b_1 \\ \dots \\ b_m \end{pmatrix}.$$

С помощью теории элементарных делителей матрицы эта задача также сводится к применению алгоритма Евклида. Элементарным преобразованием над \mathbb{Z} строк матрицы назовем преобразование, при котором к некоторой строке прибавляют другую, умноженную на целое число, а остальные строки не меняют. Проверяется, что применение такого преобразования эквивалентно умножению исходной матрицы слева на некоторую матрицу $U = E_{ij} = E + \lambda e_{ij}$ из $SL_m(\mathbb{Z})$ (соотв. $SL_n(\mathbb{Z})$) (целочисленную матрицу с определителем, равным 1). Аналогичное преобразование столбцов равносильно умножению матрицы справа на $V \in SL_m(\mathbb{Z})$

Применение нескольких таких преобразований с элементарными матрицами приводит матрицу A к виду UAV , а целочисленные решения соответствующей системы уравнений

$$UAVy = Ub \quad (3.15)$$

и исходной системы (3.14) взаимно однозначно соответствуют друг другу по формуле $x = Vy$. Теперь наибольший общий делитель d_1 элементов матрицы A можно найти повторным применением алгоритма Евклида к ее элементам $a_{i,j}$, используя элементарные преобразования строк и столбцов и при необходимости меняя знак строки так, что преобразованная матрица A' примет вид

$$D = \begin{pmatrix} d_1 & 0 & 0 & \dots & 0 \\ 0 & d_2 & 0 & \dots & 0 \\ \dots & \dots & \ddots & \dots & 0 \\ 0 & 0 & \dots & d_r & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix} = UAV. \quad (3.16)$$

Теперь мы получаем решение преобразованной (а поэтому и исходной) целочисленной системы линейных уравнений: $d_i y_i = c_i$, $c = Ub$ для $i \leq r$, $c_i = 0$ для остальных i , при этом y_i принимают произвольные целые значения. Критерий совместности над \mathbb{Z} состоит в том, что $d_i | c_i$ для всех $i \leq r$, и $c_i = 0$ для остальных i .

Числа d_i называются элементарными делителями матрицы A . Произведения $d_1 \cdots d_i$ совпадают с наибольшими общими делителями всех миноров порядка i матрицы A и $d_i | d_{i+1}$.

Отсюда следует и такая формулировка критерия совместности над \mathbb{Z} системы (3.14): для этого необходимо и достаточно, чтобы была разрешима соответствующая система сравнений

$$Ax \equiv b \pmod{N}$$

по любому натуральному модулю $N > 2$. Критерий такого рода называется принципом Минковского — Хассе и он часто встречается в задачах диофантовой геометрии.

4 Уравнения второй степени.

4.1 Квадратичные формы и квадратики

Для диофантова уравнения

$$f(x_1, x_2, \dots, x_n) = \sum_{i,j}^n a_{ij} x_i x_j + \sum_{i=1}^n b_i x_i + c = 0. \quad (4.17)$$

находить целочисленные решения значительно труднее, чем рациональные, хотя и эта задача уже нетривиальна. Известный пример связан с рациональной параметризацией окружности $x^2 + y^2 = 1$: по формулам универсальной подстановки

$$x = \frac{2t}{1+t^2}, y = \frac{1-t^2}{1+t^2} \quad (x = \cos \varphi, y = \sin \varphi, t = \tan(\frac{\varphi}{2})). \quad (4.18)$$

из которой следует описание всех примитивных пифагорейских троек (X, Y, Z) , т.е. натуральных решений $X^2 + Y^2 = Z^2$ с $(X, Y, Z) = 1$ по формулам: $X = 2uv$, $Y = u^2 - v^2$, $Z = u^2 + v^2$, где $u > v > 0$ взаимно простые числа противоположной чётности. Для этого надо в формулах (4.18) положить $t = u/v$.

Вообще, при отыскании рациональных решений уравнения (4.17) удобно перейти к квадратичной форме

$$\begin{aligned} F(X_0, X_1, \dots, X_n) &= \sum_{i,j=0}^n f_{ij} X_i X_j \\ &= \sum_{i,j=1}^n f_{ij} X_i X_j + 2 \sum_{i=1}^n f_{i0} X_i X_0 + f_{00} X_0^2, \end{aligned} \quad (4.19)$$

где $f_{ij} = f_{ji} = a_{ij}/2$ для $1 \leq i < j \leq n$ и $f_{0i} = f_{i0} = b_i/2$ с $i = 1, 2, \dots, n$, $f_{00} = c$. Для этого надо заменить неоднородные координаты x_1, \dots, x_n на однородные X_0, \dots, X_n по формулам $X_i = x_i X_0$ ($i = 1, 2, \dots, n$). Квадратичная форма $F(X)$ является однородным многочленом второй степени, который удобно записывать в матричной форме

$$F(X) = X^t A_F X, \quad X^t = (X_0, X_1, \dots, X_n),$$

где $A_F = (f_{ij})$ матрица коэффициентов. Если существует ненулевое рациональное решение $F(X) = 0$, то говорят, что F представляет нуль над полем рациональных чисел. Это уравнение

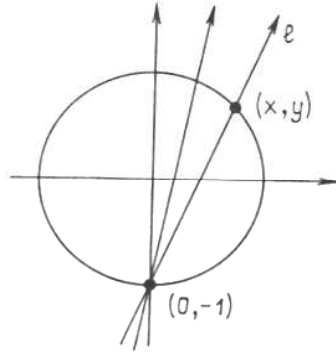


Рис. 1:

определяет квадрику Q_F , которую мы будем рассматривать как гиперповерхность в комплексном проективном пространстве \mathbb{CP}^n :

$$Q_F = \{(z_0 : z_1 : \dots : z_n) \in \mathbb{CP}^n \mid F(z_0, z_1, \dots, z_n) = 0\}.$$

Ненулевое рациональное решение $F(X) = 0$ определяет точку X_0 на квадрике Q_F . Остальные рациональные точки (рациональные решения) легко найти: они совпадают с точками пересечения квадрики Q_F со всевозможными прямыми, выходящими из X_0 и определенными над \mathbb{Q} (т.е. в направлении вектора с рациональными координатами). Прямая проходящая через X^0 и Y^0 состоит из точек $uX^0 + vY^0$. Уравнение $F(uX^0 + vY^0) = 0$ сводится к

$$uv \sum_{i=1}^n \frac{\partial F}{\partial X_i}(X^0) Y_i^0 + v^2 F(Y^0) = 0.$$

Надо только, чтобы точка X^0 не была «вершиной» на Q_F , т.е. $\frac{\partial F}{\partial X_i}(X^0) \neq 0$ хотя бы для одного i . В этом случае, для любого Y^0 находится точка пересечения Q_F с этой прямой:

$$v = -u \sum_{i=1}^n \frac{\partial F}{\partial X_i}(X^0) Y_i^0 / F(Y^0). \quad (4.20)$$

(Если $F(Y^0) = 0$ то Y^0 уже на Q_F). Примером рассмотренной конструкции, записанным в неоднородных координатах, являются формулы (4.18): чтобы найти все пары (x, y) рациональных чисел, для которых $x^2 + y^2 = 1$, рассмотрим прямую l с угловым коэффициентом t , проходящую через точки $(0, -1)$ и (x, y) : $y + 1 = tx$.

При нахождении рациональных решений уравнения

$$F(X_0, X_1, \dots, X_n) = 0 \quad (4.21)$$

(с квадратичной формой F в (4.19)) над \mathbb{Q} можно считать, что форма F – диагональна: метод Лагранжа выделения полных квадратов дает замену переменных $X = CY$ с рациональной невырожденной матрицей $C \in M_{n+1}(\mathbb{Q})$.

Для однородных уравнений типа (4.21) нет существенной разницы между их целочисленными и рациональными решениями: после умножения на подходящее целое число любое

рациональное решение становится целочисленным, и его можно считать примитивным, т. е. имеющим взаимно простые в совокупности координаты. Наиболее фундаментальным фактом теории квадратичных форм над полем рациональных чисел является следующий результат.

4.2 Принцип Минковского—Хассе для квадратичных форм.

Теорема 4.1 *Целочисленная квадратичная форма $F(x_1, x_2, \dots, x_n)$ ранга n представляет нуль над полем рациональных чисел тогда и только тогда, когда для всех натуральных чисел N , сравнение $F(x_1, \dots, x_n) \equiv 0 \pmod{N}$ имеет примитивное решение и форма F представляет нуль над полем вещественных чисел (т. е. она неопределенная).*

См. [BS85], глава 1. Конечно, утверждение «только тогда» тривиально.

Приведем красивое доказательство этой теоремы для случая, рассмотренного Лежандром ([BS85]): Пусть

$$F = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 \quad (a_1a_2a_3 \neq 0).$$

Неопределенность формы F означает, что не все коэффициенты F одного знака. Умножив форму при необходимости на -1 мы приходим к случаю, когда два коэффициента положительны, а один отрицателен. Кроме того, мы можем считать эти числа целыми, свободными от квадратов и взаимно простыми в совокупности, так как их можно сократить на наибольший общий делитель. Далее, если, например, a_1 и a_2 имеют общий простой делитель p , то, умножив форму на p и взяв px и py за новые переменные, мы получим форму с коэффициентами a_1/p , a_2/p и pa_3 . Повторяя этот процесс несколько раз, мы заменим нашу форму формой вида

$$ax^2 + by^2 - cz^2. \quad (4.22)$$

в которой целые положительные числа a, b, c попарно взаимно просты (и свободны от квадратов). Пусть теперь p какой-нибудь простой делитель числа c , отличный от 2.

Можно показать, что поскольку для исходной формы существует примитивное решение сравнения $F \equiv 0 \pmod{p^l}$ для любого $l \geq 1$, то сравнение $ax^2 + by^2 \equiv 0 \pmod{p}$ имеет нетривиальное решение (x_0, y_0) . Следовательно, можно предполагать, что $y_0 \neq 0$, и выполняется разложение на множители

$$ax^2 + by^2 \equiv ay_0^{-2}(xy_0 + yx_0)(xy_0 - yx_0) \pmod{p}.$$

Аналогичные разложения имеют место по модулю нечетных p , делящих коэффициенты a и b , а при $p = 2$ выполняется сравнение

$$ax^2 + by^2 - cz^2 \equiv (ax + by - cz)^2 \pmod{2}.$$

Таким образом, для любого простого числа $p \mid 2abc$ существуют линейные формы $L^{(p)}$, $M^{(p)}$ от x, y, z с целыми коэффициентами, такие, что $F \equiv L^{(p)}M^{(p)} \pmod{p}$. Теперь с помощью китайской теоремы об остатках найдем такие линейные формы L (соотв. M) с целыми коэффициентами, сравнимыми с $L^{(p)}$ (соотв. $M^{(p)}$) \pmod{p} для всех $p \mid abc$, и мы получим

$$ax^2 + by^2 + cz^2 \equiv L(x, y, z)M(x, y, z) \pmod{abc}. \quad (4.23)$$

Будем придавать переменным x, y, z целые значения, удовлетворяющие условиям

$$0 \leq x < \sqrt{bc}, \quad 0 \leq y < \sqrt{ac}, \quad 0 \leq z < \sqrt{ab}. \quad (4.24)$$

Если исключить из рассмотрения тривиальный случай $a = b = c = 1$, то не все числа $\sqrt{bc}, \sqrt{ac}, \sqrt{ab}$ целые и число троек (x, y, z) , удовлетворяющих условиям (4.24), строго больше чем объём $\sqrt{bc}\sqrt{ac}\sqrt{ab} = abc$. Следовательно, для некоторых двух различных троек линейная форма L принимает одно и то же значение $\text{mod } abc$, откуда в силу линейности формы имеем

$$L(x_0, y_0, z_0) \equiv 0 \pmod{abc} \quad (4.25)$$

для некоторого решения $|x_0| \leq \sqrt{bc}$, $|y_0| \leq \sqrt{ac}$, $|z_0| \leq \sqrt{ab}$. Поэтому

$$ax_0^2 + by_0^2 - cz_0^2 \equiv 0 \pmod{abc} \quad (4.26)$$

и имеют место неравенства

$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc.$$

Таким образом, справедливо одно из двух равенств

$$ax_0^2 + by_0^2 - cz_0^2 = 0 \quad (4.27)$$

или же

$$ax_0^2 + by_0^2 - cz_0^2 = abc. \quad (4.28)$$

В случае (4.27) теорема доказана; если же выполнено равенство (4.28), то доказательство следует из тождественного преобразования

$$a(x_0z_0 + by_0)^2 + b(y_0z_0 - ax_0)^2 - c(z_0^2 + ab)^2 = 0.$$

В формулировке Лежандра диофантово уравнение $ax^2 + by^2 - cz^2 = 0$ имеет нетривиальное целочисленное решение в том и только в том случае, когда классы вычетов

$$bc \pmod{a}, \quad ac \pmod{b}, \quad -ab \pmod{c}$$

являются квадратами.

Можно доказать, что рациональная квадратичная форма ранга ≥ 5 всегда представляет нуль над \mathbb{Q} .

В общем случае существуют эффективные методы (основанные на принципе Минковского – Хассе для квадратичных форм), чтобы установить, представляет ли квадратичная форма рациональный нуль. Эти методы основаны на информации, которую можно извлечь из вещественных и конгруэнциальных рассмотрений, и используют символ Гильберта.

4.3 Символ Гильберта.

В этом пункте мы допускаем значение $p = \infty$, и считаем тогда, что $\mathbb{Q}_\infty = \mathbb{R}$. Символ Гильберта (символ норменного вычета)

$$(a, b) = \left(\frac{a, b}{p} \right) = \left(\frac{a, b}{p} \right) = (a, b)_p$$

для $a, b \in \mathbb{Q}_p^\times$ определяется равенством

$$(a, b) = \begin{cases} 1, & \text{если форма } ax^2 + by^2 - z^2 \text{ имеет} \\ & \text{нетривиальное решение в } \mathbb{Q}_p; \\ -1, & \text{в противном случае.} \end{cases}$$

Ясно, что (a, b) зависит только от a и b по модулю квадратов в \mathbb{Q}_p . Существует несимметричная форма этого определения. Именно, $(a, b) = 1$ тогда и только тогда, когда

$$a = z^2 - by^2 \text{ для некоторых } y, z \in \mathbb{Q}_p. \quad (4.29)$$

Действительно, из соотношения (4.29) следует, что $(1, y, z)$ нетривиальный нуль квадратичной формы $ax^2 + by^2 - z^2$. Наоборот, если, (x_0, y_0, z_0) некоторый нетривиальный нуль, то остальные нули получаются с помощью геометрического приема проведения секущих через точку (x_0, y_0, z_0) с направляющим вектором, имеющим координаты из \mathbb{Q}_p . Поэтому можно считать, что $x_0 \neq 0$. Поэтому $(y_0/x_0, z_0/x_0)$ удовлетворяют соотношению (4.29).

Локальные свойства символа Гильберта:

$$\text{а) } (a, b) = (b, a); \quad (4.30)$$

$$\text{б) } (a_1 a_2, b) = (a_1, b)(a_2, b), \quad (a, b_1 b_2) = (a, b_1)(a, b_2); \quad (4.31)$$

$$\text{в) } \text{если } (a, b) = 1 \text{ для всех } b, \text{ то } a \in \mathbb{Q}_p^{\times 2}; \quad (4.32)$$

$$\text{г) } (a, -a) = 1 \text{ для всех } a; \quad (4.33)$$

$$\text{д) } \text{если } p \neq 2, \infty \text{ и } |a|_p = |b|_p = 1, \text{ то } (a, b) = 1. \quad (4.34)$$

В частности, при фиксированном b , все a , для которых $(a, b) = 1$ образуют группу по умножению. Уравнение (4.29) выражает тот факт, что a является нормой из квадратичного расширения $\mathbb{Q}_p(\sqrt{b})/\mathbb{Q}_p$ (cf. [BS85], [Se70]).

Вычисление символа Гильберта позволяет полностью решить «глобальный» вопрос о представлении нуля рациональными квадратичными формами (с помощью теоремы Минковского – Хассе). Если, скажем,

$$Q(x, y, z) = ax^2 + by^2 + cz^2 \quad (a, b, c \in \mathbb{Q}, c \neq 0), \quad (4.35)$$

то форма (4.35) представляет нуль над полем \mathbb{Q} тогда и только тогда, когда выполняется равенство $(-a/c, -b/c)_p = 1$ для всех p (включая $p = \infty$). 1. Этот критерий является весьма эффективным, так как $|a|_p = |b|_p = 1$ для почти всех p причем в этом случае $(a, b)_p = 1$ если $p \neq 2, \infty$ согласно свойству (4.34). Выпишем теперь таблицу для $(a, b)_p$:

Таблица 1: Символ Гильберта для $p > 2$. Здесь v обозначает такое число $v \in \mathbb{Z}$, что $\left(\frac{v}{p}\right) = -1$, а $\varepsilon = 1$ если $-1 \in \mathbb{Q}_p^{\times 2}$ (т. е. если $p \equiv 1 \pmod{4}$), а $\varepsilon = -1$ в противном случае

b	a	1	v	p	pv
1		+1	+1	+1	+1
v		+1	+1	-1	-1
p		+1	-1	ε	$-\varepsilon$
pv		+1	-1	$-\varepsilon$	ε

Глобальное свойство символа Гильберта (формула произведения). Пусть $a, b \in \mathbb{Q}^\times$. Тогда $(a, b)_p = 1$ для почти всех p и

$$\prod_{p \text{ including } \infty} (a, b)_p = 1. \quad (4.36)$$

Таблица 2: Символ Гильберта в случае $p = 2$.

a	1	5	-1	-5	2	10	-2	-10
b								
1	+1	+1	+1	+1	+1	+1	+1	+1
5	+1	+1	+1	+1	-1	-1	-1	-1
-1	+1	+1	-1	-1	+1	+1	-1	-1
-5	+1	+1	-1	-1	-1	-1	+1	+1
2	+1	-1	+1	-1	+1	-1	+1	-1
10	+1	-1	+1	-1	-1	+1	-1	+1
-2	+1	-1	-1	+1	+1	-1	-1	+1
-10	+1	-1	-1	+1	-1	+1	+1	-1

Формула (4.36) равносильна квадратичному закону взаимности. Действительно, по свойству (4.34) имеем $|a|_p = |b|_p = 1$ для почти всех p , и в этом случае $(a, b)_p = 1$ for $p \neq 2, \infty$ в силу (4.34). Обозначим левую часть равенства (4.36) через $f(a, b)$. По свойствам (4.31) имеем

$$\begin{aligned} f(a_1 a_2, b) &= f(a_1, b) f(a_2, b), \\ f(a, b_1 b_2) &= f(a, b_1) f(a, b_2), \end{aligned}$$

и можно проверить, что $f(a, b) = 1$ когда a и b пробегают множество образующих группы \mathbb{Q}^\times : $-1, 2, -q$ нечетное простое число.

Отметим также следующее глобальное свойство нормирований $|\cdot|_p$, аналогичное свойству (4.36):

Формула произведения для нормирований. Пусть $a \in \mathbb{Q}^\times$, тогда $|a|_p = 1$ для почти всех простых чисел p , и

$$\prod_{p \text{ including } \infty} |a|_p = 1. \quad (4.37)$$

Действительно, если $a \in \mathbb{Q}^\times$, то

$$a = \pm \prod_{p \neq \infty} p^{v_p(a)},$$

где $v_p(a) \in \mathbb{Z}$ и $v_p(a)$ для почти всех p . Тогда

$$|a|_p = p^{-v_p(a)} \text{ (для } p \neq \infty),$$

$$|a|_\infty = \prod_{p \neq \infty} p^{v_p(a)}.$$

5 Кубические уравнения и эллиптические кривые

5.1 Проблема существования рационального решения.

Для целочисленных кубических форм $F(X, Y, Z)$ от трех переменных уже не известно никакого общего алгоритма, позволяющего установить существование нетривиального решения над \mathbb{Q} ,

хотя изучено большое число конкретных уравнений, например уравнений вида

$$aX^3 + bY^3 + cZ^3 = 0.$$

Оказывается, для кубических форм перестает, вообще говоря, выполняться принцип Минковского – Хассе: уравнение $3X^3 + 4Y^3 + 5Z^3 = 0$ не имеет нетривиальных решений в целых числах, хотя имеет вещественные решения, и для всех натуральных $N > 1$ сравнение $3X^3 + 4Y^3 + 5Z^3 = 0 \pmod N$ имеет примитивное решение. Нарушение принципа Минковского–Хассе может быть измерено численно при помощи группы *Шафаревича–Тэйта*, см. главу 5 книги [Ма-Ра05].

5.2 Сложение точек на кубической кривой.

Кубическая форма $F(X, Y, Z)$ задает кривую \mathcal{C} на проективной плоскости \mathbb{P}^2 :

$$\mathcal{C} = \{(X : Y : Z) \mid F(X, Y, Z) = 0\}. \quad (5.38)$$

причем мы считаем, что координаты в форме (5.38) — комплексные числа. Если на \mathcal{C} лежит хотя бы одна рациональная точка O , и кривая \mathcal{C} невырождена, то можно найти такую обратимую замену координат (над полем \mathbb{Q}) после которой форма F примет вид

$$Y^2Z - X^3 - aXZ^2 - bZ^3 \quad (a, b \in \mathbb{Q}). \quad (5.39)$$

(вейерштрассова форма), причем точка O перейдет в решение $(0 : 1 : 0)$ для формы (5.39), а условие невырожденности для кривой (5.39) станет эквивалентно тому, что $4a^3 + 27b^2 \neq 0$.

Невырожденная кубическая кривая, имеющая рациональную точку, называется эллиптической кривой. В неоднородных координатах $x = X/Z, y = Y/Z$ уравнение кривой $F = 0$ примет вид

$$y^2 = x^3 + ax + b, \quad (5.40)$$

причем кубический многочлен справа не имеет кратных комплексных корней (его дискриминант отличен от нуля), а точка $O = (0 : 1 : 0)$ в этой записи станет бесконечно удаленной точкой. Существует красивый геометрический способ превратить множество рациональных точек \mathcal{C} на такой кривой в абелеву группу с нейтральным элементом O («метод секущих и касательных»), см. [Sha88], [Ма-Ра05]. Если $P, Q \in \mathcal{C}(\mathbb{Q})$, то проводим через P, Q проективную прямую, пересекающую \mathcal{C} в однозначно определенной третьей точке $P' \in \mathcal{C}(\mathbb{Q})$. затем проводим прямую через P' и O , а точку ее пересечения с \mathcal{C} назовем суммой точек $P + Q$. Аналогично определяется точка $2P$ если использовать касательную, проходящую через точку P .

Если $P = (x_1, y_1)$, $Q = (x_2, y_2)$ в неоднородных координатах, причем $x_1 \neq x_2$, то $P + Q = (x_3, y_3)$, где

$$\begin{aligned} x_3 &= -x_1 - x_2 + \left(\frac{y_1 - y_2}{x_1 - x_2} \right)^2, \\ y_3 &= \frac{y_1 - y_2}{x_1 - x_2} (x_1 - x_3) - y_1. \end{aligned} \quad (5.41)$$

Если же $P = Q$, то

$$x_3 = -2x_1 + \left(\frac{3x_1^2 + a}{2y_1} \right)^2, \quad y_3 = \frac{3x_1^2 + a}{2y_1} (x_1 - x_3) - y_1. \quad (5.42)$$

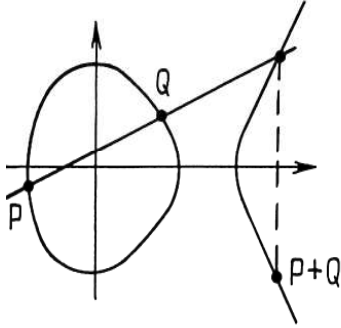


Рис. 2:

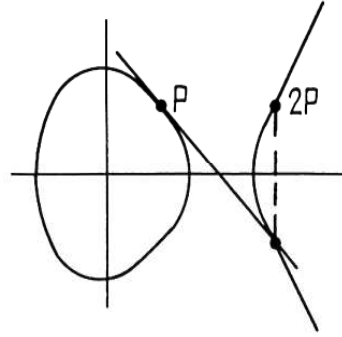


Рис. 3:

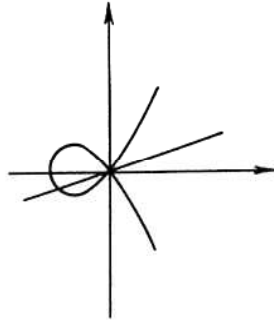


Рис. 4:

Если $x_1 = x_2$, но $y_1 = -y_2$ то точка $P + Q = O$, бесконечно удаленная; она выбрана нейтральным элементом группового закона, поэтому в данном случае $P = -Q$.

Описанный метод дает возможность размножать рациональные точки, mP , $m \in \mathbb{Q}$ рассматривая кратные mP , $m \in \mathbb{Q}$, а также их суммы с другими точками Q (если таковые имеются).

Для вырожденных кубических кривых описанный метод неприменим. Пусть, к примеру,

$$C: y^2 = x^2 + x^3, \quad (5.43)$$

кривая, изображенная на рис. 4. Тогда любая прямая, проходящая через точку $(0,0)$ имеет лишь одну точку пересечения с кривой C : если уравнение прямой $y = tx$ то мы получаем из уравнения, что $x^2(t^2 - x - 1) = 0$. Корень $t = 0$ соответствует точке $(0,0)$; $x = 0$, кроме того, мы имеем еще один корень $x = t^2 - 1$. Из уравнения прямой мы получаем, что $y = t(t^2 - 1)$. Поэтому, хотя и нельзя определить групповой закон, как выше, мы находим все рациональные точки на C с помощью рациональной параметризации: $(x, y) = (t^2 - 1, t(t^2 - 1))$.

Вообще, кривая, допускающая параметризацию с помощью некоторых рациональных функ-

ций с коэффициентами из поля K , называется рациональной над K .

5.3 Строение группы рациональных точек на кубической кривой

Наиболее выдающаяся особенность метода секущих и касательных — это возможность сводить нахождение всех рациональных решений кубического уравнения (5.40) к нахождению лишь конечного их числа. Точнее, имеет место следующий результат.

Теорема 5.1 (теорема Морделла) *Абелева группа $\mathcal{C}(\mathbb{Q})$ конечно порождена.*

(см. [Cas66], и приложение Ю. И. Манина к [Mum74]). Согласно теореме о строении конечно порожденных абелевых групп имеется разложение

$$\mathcal{C}(\mathbb{Q}) \cong \Delta \times \mathbb{Z}^r$$

где Δ — конечная подгруппа всех точек кручения, и \mathbb{Z}^r — прямая сумма бесконечных циклических групп; число r называют рангом кривой \mathcal{C} над \mathbb{Q} .

О группе кручения Δ уже давно было кое-что известно. Так, Нагелль и позднее Лутц получили следующий интересный результат, дающий одновременно метод для явного определения точек кручения конкретных кривых: если $P = (x_P, y_P)$ — рациональная точка кручения на кривой, заданной уравнением $y^2 = x^3 + ax + b$, то её координаты x_P и y_P являются целыми числами, причём y_P или равно 0, или y_P^2 равен какому-нибудь делителю дискриминанта $D = -4a^3 - 27b^2$ данной кривой.

Б. Мазур доказал в 1976 г., что подгруппа Δ кручения над \mathbb{Q} может быть изоморфна лишь одной из пятнадцати групп:

$$\mathbb{Z}/m\mathbb{Z} \ (m \leq 10, m = 12), \ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \ (n \leq 4), \quad (5.44)$$

причем все возможности реализуются (см. [?], глава 6).

Вычисление ранга r остаётся открытой проблемой.

Примеры. 1) Кривая \mathcal{C} задается уравнением

$$y^2 + y = x^3 - x$$

целочисленное решение которого даёт пример, когда произведение двух последовательных целых чисел равно произведению некоторых других трёх последовательных чисел. Тогда группа Δ тривиальна, а группа точек $\mathcal{C}(\mathbb{Q})$ (с бесконечно удаленной точкой в качестве нейтрального элемента) является бесконечной циклической группой, причем в качестве её образующей можно взять точку $P = (0, 0)$. Точки вида mP указаны на рис. 5.

2) Пусть кривая \mathcal{C} задана уравнением

$$y^2 + y = x^3 - 7x + 6.$$

Тогда $\mathcal{C}(\mathbb{Q}) \cong \mathbb{Z}^3$, а свободные образующие этой группы даются решениями $(1, 0)$, $(2, 0)$, $(0, 2)$, см. [BGZ85].

3) Кривая $\mathcal{C} : y(y + 1) = x(x - 1)(x + 2)$ имеет ранг, равный двум, а кривая $r = 2$; for $\mathcal{C} : y(y + 1) = x(x - 1)(x + 4)$, имеет ранг $r = 2$, ср. с уравнением кривой ранга 1 из примера 1.

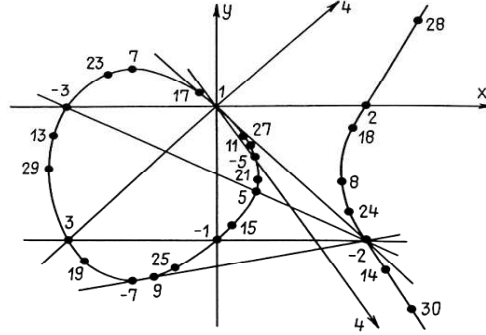


Рис. 5:

4) Рассмотрим кривую $y^2 = x^3 + px$, $p = 877$. Можно показать (см. ссылки в), что образующая по модулю кручения группы рациональных точек на этой кривой имеет x -координату

$$x = \frac{375494528127162193105504069942092792346201}{6215987776871505425463220780697238044100}.$$

Этот пример дает определенное представление о трудностях «наивного» элементарного подхода для нахождения точек бесконечного порядка на эллиптических кривых, см. [Coa84].

5.4 Кубические сравнения по простому модулю.

Пусть p простое число, и $F(X_0, X_1, X_2)$ — кубическая форма, невырожденная по модулю p . Это значит, что для любого поля $F \supset \mathbb{F}_p$ (т. е. поля характеристики p), следующие формы степени 3 и 2:

$$\overline{F}, \frac{\partial \overline{F}}{\partial X_i} (i = 0, 1, 2)$$

не имеют общих нетривиальных нулей над K , где \overline{F} обозначает форму, полученную из F рассмотрением ее коэффициентов по модулю p .

Как над полем рациональных чисел, простые алгебро-геометрические идеи можно применить и к полю K положительной характеристики. В этом случае нормальная форма становится несколько более сложной. Сделав замену проективных координат и перейдя к неоднородной форме записи, мы всегда можем привести уравнение $F = 0$ к виду

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

где $a_1, a_2, a_3, a_4, a_6 \in K$ и

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \neq 0,$$

где

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

(Обозначения Тэйта). Также используется обозначение $j = \frac{c_4^3}{\Delta}$, где

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Затем это уравнение может быть еще упрощено при помощи преобразований вида $x \mapsto u^2x' + r$, $y \mapsto u^3y' + su^2x'r + t$ и получается следующее (см.. [Kob87]):

1) Если $p \neq 2, 3$, то

$$y^2 = x^3 + a_4x + a_6 \text{ с } \Delta = -16(4a_4^3 + 27a_6^2) \neq 0. \quad (5.45)$$

2) Если $p = 2$ условие $j = 0$ равносильно тому, что $a_1 = 0$, и уравнение преобразуется к следующему виду: если $a_1 \neq 0$ (т.е. $j \neq 0$), то, выбирая подходящие r, s, t мы можем получить $a_1 = 1, a_3 = 0, a_4 = 0$, и уравнение принимает вид

$$y^2 + xy = x^3 + a_2x^2 + a_6, \quad (5.46)$$

где условие гладкости задается просто неравенством $\Delta \neq 0$. Предположим теперь, что $a_1 = 0$ (т.е. $j = 0$). В этом случае уравнение преобразуется в

$$y^2 + a_3y = x^3 + a_4x + a_6, \quad (5.47)$$

и условие гладкости в этом случае задается неравенством $a_3 \neq 0$.

3) Если $p = 3$, то

$$y^2 = x^3 + a_2x^2 + a_4x + a_6, \quad (5.48)$$

(в этом случае кратные корни также недопустимы). В однородных координатах во всех случаях добавляется «бесконечно удаленное решение» $O = (0 : 1 : 0)$.

Как посчитать число решений таких кубических сравнений $F \equiv 0 \pmod{p}$? Ясно, во-первых, что число этих решений, образующих вместе с точкой O абелеву группу порядок которой не превосходит $2p + 1$, так как для каждого такого x найдутся не больше двух значений y . Однако лишь половина элементов из $(\mathbb{F}_p)^\times$ являются квадратами, поэтому можно ожидать, что лишь в половине случаев из элемента можно извлечь квадратный корень y (предположив, что элементы $x^3 + ax + b$ разбросаны случайно в поле \mathbb{F}_p).

Более точно, пусть $\chi(x) = \left(\frac{x}{p}\right)$ — символ Лежандра, определение которого означает, что число решений уравнения $y^2 = u$ в \mathbb{F}_p равно $1 + \chi(u)$. Тогда мы получаем следующую формулу для числа решений кубического сравнения:

$$\begin{aligned} \text{Card } \mathcal{C}(\mathbb{F}_p) &= 1 + \sum_{x \in \mathbb{F}_p} (1 + \chi(x^3 + ax + b)) \\ &= p + 1 + \sum_{x \in \mathbb{F}_p} \chi(x^3 + ax + b). \end{aligned}$$

Коблиц в [Kob87] сравнивает взятие суммы со «случайным блужданием», при котором делается шаг вперед, если $\chi(x^3 + ax + b) = 1$, и шаг назад, если $\chi(x^3 + ax + b) = -1$. Из теории вероятностей известно, что расстояние от исходной точки после p шагов при случайном блуждании будет иметь порядок \sqrt{p} . И действительно, это так: сумма всегда ограничена величиной $2\sqrt{p}$.

Теорема 5.2 (теорема Хассе) Пусть $N_p = \text{Card } \mathcal{C}(\mathbb{F}_p)$, тогда

$$|N_p - (p + 1)| \leq 2\sqrt{p}.$$

Элементарное доказательство этого факта было дано Ю.И.Маниным в 1956.

5.5 От сравнений к рациональным точкам: гипотеза Бёрча и Суиннертона–Дайера

Знаменитый пример связывающий локальную и глобальную информацию, даётся гипотезой Бёрча и Суиннертона–Дайера для эллиптических кривых. Эта гипотеза принадлежит к числу Семи Проблем Тысячелетия института CLAY, а за её решение предложен приз в миллион долларов!

Эта открытая проблема обсуждается также в статье Уайлса [WilesBSD].

5.5.1 Гипотеза БСД

(см. изложение в [Stein], главы 8 и 9) Пусть E эллиптическая кривая над \mathbb{Q} заданная уравнением

$$y^2 = x^3 + ax + b$$

с $a, b \in \mathbb{Z}$. Для $p \nmid \Delta = -16(4a^3 + 27b^2)$, положим $a_p = p + 1 - \#E(\mathbb{Z}/p\mathbb{Z})$. Пусть

$$L(E, s) = \prod_{p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \quad (5.49)$$

ряд Дирихле, сходящийся абсолютно при $\operatorname{Re}(s) > \frac{3}{2}$ в силу теоремы Хассе (теорема 5.2).

Теорема 5.3 (Брёй, Конрад, Дайамонд, Тэйлор, Уайлс)

Функция $L(E, s)$ пролжается до аналитической функции на всей комплексной плоскости \mathbb{C} .

(см. Breuil, Conrad, Diamond, Taylor, Wiles, а также ссылки в [Ma-Pa05]).

Гипотеза 5.4 (Бёрча и Суиннертона–Дайера) *Разложение Тэйлора функции $L(E, s)$ в $s = 1$ имеет вид*

$$L(E, s) = c(s-1)^r + \text{члены высшей степени}$$

с $c \neq 0$ и $E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}}$.

Специальный случай гипотезы БСД утверждает, что $L(E, 1) = 0$ тогда и только тогда, когда $E(\mathbb{Q})$ бесконечна, в частности утверждение “ $L(E, 1) = 0$ влечёт, что группа $E(\mathbb{Q})$ бесконечна”.

5.5.2 Что известно о гипотезе БСД

В статье [WilesBSD] обсуждается история следующего результата:

Теорема 5.5 (Гросс, Колывагин, Загир и др.) *Предположим, что*

$$L(E, s) = c(s-1)^r + \text{члены высшей степени}$$

с $r \leq 1$. Тогда гипотеза Бёрча и Суиннертона–Дайера справедлива для E , то есть $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$.

5.5.3 Вычисления с эллиптическими кривыми

Опишем, как использовать компьютер для приближённого вычисления ранга r кривой.

Пусть E — эллиптическая кривая над полем \mathbb{Q} , определённая обобщённым уравнением Вейерштрасса

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Напечатав `e = ellinit([a1,a2,a3,a4,a6])`, мы зададим эту кривую на компьютерной системе PARI (см. [BBBCO]). Например, напечатав `e = ellinit([0,0,1,-7,6])`, мы получим на PARI кривую $y^2 + y = x^3 - 7x + 6$. Приведём пример вычисления на PARI:

5.5.4 С чего начать вычисления на PARI-GP

Документация

Документация для PARI доступна по адресу:

<http://pari.math.u-bordeaux.fr>

Вот некоторая документация для PARI:

1. **Installation Guide:** Помощь по установке PARI на компьютере.
2. **Tutorial:** Превосходный вводный текст на 42 страницы, который начинается с $2 + 2$.
3. **User's Guide:** Подробное описание всех функций на 226 страницы.
4. **Reference Card:** 4 страницы (очень полезная сводка команд и их применения)

```
gp > factor(2^256+1)
%1=
[1238926361552897 1]

[93461639715357977769163558199606896584051237541638188580280321 1]

*** last result computed in 14,501 ms.
```

5.5.5 Как вычислить $L(E, s)$ на компьютере

Пусть E — эллиптическая кривая над полем \mathbb{Q} , определённая обобщённым уравнением Вейерштрасса

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Имеется много возможностей для выбора уравнения Вейерштрасса определяющих эллиптическую кривую E с точностью до изоморфизма. Среди этих уравнений имеется наилучшее (минимальное), то есть с наименьшим дискриминантом. Пример вычисления на PARI:

```
? E = ellinit([0,0,0,-43,166]);
? E.disc
%61 = -6815744
? E = ellchangecurve(E,ellglobalred(E)[2])
%62 = [1, -1, 1, -3, 3, ...]
? E.disc
%63 = -1664
```

Таким образом, уравнение $y^2 + xy + y = x^3 - x^2 - 3x + 3$ “лучше”, чем $y^2 = x^3 - 43x + 166$.

ПРЕДУПРЕЖДЕНИЕ: Некоторые важные функции на PARI дают лишь тогда верный результат, когда уравнение кривой выбрано наилучшим (минимальным). Это относится к таким функциям, как `elltors`, `ellap`, `ellak`, и `ellseries`.

Напечатав `e = ellinit([0,0,1,-7,6])`, мы получим на PARI кривую $y^2 + y = x^3 - 7x + 6$. Напечатав `ellglobalred(e)` мы найдём, что уравнение минимальное и что кондуктор равен дискриминанту 5077.

5.5.6 Приближённое вычисление ранга

Опишем метод приближённого вычисления ранга кривой на PARI. Можно, например, приближённо вычислять значения $L^{(r)}(E, 1)$ для $r = 0, 1, 2, 3, \dots$, до тех пор, пока не получится ненулевое значение. Этот метод описан в книге Дж.Кремоны (см. [Cremona]).

Предложение 5.6 Пусть $L(E, s) = c(s-1)^r + \text{члены высшей степени}$. Тогда

$$\lim_{s \rightarrow 1} (s-1) \frac{L'(E, s)}{L(E, s)} = r.$$

Таким образом, ранг r вычисляется как “точный” предел при $s \rightarrow 1$ для мероморфных функций. Известно, что этот предел является целым числом. Для кривой $y^2 + y = x^3 - 7x + 6$ можно показать, что этот предел равен 3. Теперь используем такой приём:

$$(s-1) \frac{L'(s)}{L(s)} = \frac{s-1}{L(s)} \cdot \lim_{h \rightarrow 0} \frac{L(s+h) - L(s)}{h} \approx \frac{s-1}{L(s)} \cdot \frac{L(s + (s-1)^2) - L(s)}{(s-1)^2} = \frac{L(s^2 - s + 1) - L(s)}{(s-1)L(s)}.$$

Эту формулу возможно использовать на PARI для приближённого вычисления ранга r кривой.

```
gp > e=ellinit([0,0,1,-7,6]);
gp > r(E,s) = L1 = ellseries(E,s)
L2 = ellseries(E,s^2-s+1);
(L2-L1)/((s-1)*L1);
gp > r(e,1.00001)
%2 = 3.000011487248732705286325574
gp > ##
*** last result computed in 510 ms.
```

Напомним, что $\mathcal{C}(\mathbb{Q}) \cong \mathbb{Z}^3$, а свободные образующие этой группы даются решениями $(1,0)$, $(2,0)$, $(0, 2)$, см. [BGZ85].

Джон Тэйт сделал доклад о гипотезе БСД для института Clay. Этот доклад можно посмотреть онлайн по адресу:

<http://www.msri.org/publications/ln/hosted/cmi/2000/cmiparis/index-tate.html>

Признательность автора

Искренне благодарю Эрнеста Борисовича Винберга за приглашение подготовить статью для журнала “Математическое Просвещение” 2008, посвящённого p -адическим числам и их приложениям.

Список литературы

- [BBBCO] Batut, C., Belabas, D., Bernardi, H., Cohen, H., Olivier, M.: The PARI/GP number theory system. <http://pari.math.u-bordeaux.fr>
- [BS85] Borevich, Z.I., Shafarevich, I.R. (1985): Number Theory. (in Russian). 3rd ed. Nauka, Moscow (1985). English transl.: New York/London: Academic Press, 1966.
- [Cas66] Cassels, J.W.S. (1966): Diophantine equations with special reference to elliptic curves. J. Lond. Math. Soc., 41 (1966), 193-291.
- [Coa84] Coates, J. (1984): The work of Gross and Zagier on Heegner points and the derivatives of L -series. Séminaire Bourbaki, Exp. 633, 1984.
- [Cremona] Cremona, J. *Algorithms for Elliptic Curves*
- [BGZ85] Joe P. Buhler; Benedict H. Gross; Don B. Zagier On the Conjecture of Birch and Swinnerton-Dyer for an Elliptic Curve of Rank 3 Mathematics of Computation, Vol. 44, No. 170. (Apr., 1985), pp. 473-481.
- [Kob77] Koblitz, N. (1977): p -adic numbers, p -adic analysis and zeta-functions. New York: Springer Verlag (1977).
- [Kob80] Koblitz, N. (1980): p -adic analysis: a short course on recent work. London Math. Soc. Lecture Note Ser., London: Cambridge Univ. Press (1980).
- [Kob84] Koblitz, N. (1984): Introduction to elliptic curves and modular forms. New York: Springer Verlag, 1984.
- [Kob87] Koblitz, N. (1987): A course of number theory and cryptography. New York: Springer Verlag, 1987.
- [Kum75] Kummer, E.E. (1975): Collected papers. Vol. 1. New York: Springer Verlag (1975).
- [Man96] Manin, Yu.I., *Selected papers of Yu.I. Manin*, World Scientific Series in 20th Century Mathematics, 3. World Scientific Publishing Co., Inc., River Edge, NJ, 1996. xii+600 pp.
- [Ma-Pa05] Manin, Yu.I. and Panchishkin, A.A., *Introduction to Modern Number Theory*, Encyclopaedia of Mathematical Sciences, vol. 49 (2nd ed.), Springer-Verlag, 2005, 514 p.
- [Mum74] Mumford, D. (1974): Abelian varieties. Oxford Univ. Press (1974).
- [Se70] Serre, J.-P. (1970): Cours d'arithmétique. Paris: Presses Univ. France, 1970.
- [Sha88] Shafarevich, I.R. Foundations of algebraic geometry. (In Russian). 2nd ed. Vols. 1-2. Moscow: Nauka, 1988. English transl.: Berlin-Heidelberg-New York: Springer-Verlag,
- [Stein] W. Stein, *Elementary Number Theory*, <http://modular.math.washington.edu/ent/>.
- [TaWi] TAYLOR, R. and WILES, A., *Ring theoretic properties of certain Hecke algebras*, Ann. of Math. 141 (1995), 553-572
- [WilesBSD] A. WILES, *The Birch and Swinnerton-Dyer Conjecture*, An article for the Clay Math Institute.

- [Wi95] A. WILES, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math., II. Ser. 141, No.3 (1995), 443–55.

This figure "Img3.jpg" is available in "jpg" format from:

<http://arXiv.org/ps/0709.1606v1>

This figure "Img6.jpg" is available in "jpg" format from:

<http://arXiv.org/ps/0709.1606v1>

This figure "Img7.jpg" is available in "jpg" format from:

<http://arXiv.org/ps/0709.1606v1>

This figure "Img8.jpg" is available in "jpg" format from:

<http://arXiv.org/ps/0709.1606v1>

This figure "Img9.jpg" is available in "jpg" format from:

<http://arXiv.org/ps/0709.1606v1>